UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/059,182	01/31/2002	Janne Suuronen	004770.00521	5357

22907 7590 09/03/2008

BANNER & WITCOFF, LTD.
1100 13th STREET, N.W.
SUITE 1200
WASHINGTON, DC 20005-4051

EXAMINER	
SHAW, YIN CHEN	
ART UNIT	PAPER NUMBER
2139	
MAIL DATE	DELIVERY MODE
09/03/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/059,182	SUURONEN ET AL.	
	Examiner	Art Unit	
	Yin-Chen Shaw	2139	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *05/28/2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,4-6,11,32-34,40-50,53,54 and 56-65* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1, 4-6, 11, 32-34, 40-50, 53-54, and 56-65* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This written action is responding to the amendment dated on 05/28/2008.
2. Claims 1, 4-6, 11, 32-34, 40-50, 53-54, and 56-63 are previously presented. Claims 64-65 are newly added.
3. Claims 1, 4-6, 11, 32-34, 40-50, 53-54, and 56-65 have been submitted for examination.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 1, 4, 11, 32-34, 40-50, 53, 56, 58, 60-62, and 65 are rejected under 35 U.S.C. 103(a) as being unpatentable over Fink et al. (U.S. Patent 6,496,935) and Joyce (U.S. Patent 6,519,703).

   i. *Referring to Claims 1, 49, 50, and 62:*

   As per Claim 1, Fink et al. disclose an apparatus comprising:

   a firewall **[(fig. 1)]** configured to:

   receive data packets over a first network **[Packets which are permitted to pass through gateway 15 from external network**

14 are then received by one of a plurality of protected nodes 20 (lines 335-37, Col. 5)];

classify the received data packets based on the contents of the data packets into packets of a first type and second type **[inspects the contents of such packet or packets (line 67, Col. 6). Pre-filtering module 30 also preferably features a classification engine 38, including a data processor, for at least partially analyzing the information from the packet (lines 4-6, Col. 8)]**;

Fink et al. do not expressly disclose the remaining limitations of the claim. However, Joyce discloses packets which cannot contain virus and packets which can contain a virus and the virus scanning engine for testing if the packet contains virus **[Prior to use, heuristic firewall 10B is trained to perform specific desired tasks. In this embodiment, for example, a first heuristic stage 36 is trained to recognize absolute high-confidence traffic, computer virus and Trojan signatures, denial-of-service attack signatures, and other computer security exploit signatures. After training and during use, if heuristic stage 36 clears a packet stream with a "high-confidence" rating (i.e., an analysis of the packets 22 by heuristic stage 36 results in a high level of confidence that the packet stream does not contain threats that heuristic**

stage 36 is trained to detect), buffer 24 releases the packets into a secured channel 38 directly into network 30. If heuristic stage 36 processing results in only a lesser confidence rating (i.e., a "good-confidence" rating) that threats are absent, buffer 24 releases the packets into a traditional firewall rule base 12 for standard processing. In this case, the output of traditional firewall rule base 12 is buffer 28. If heuristic stage 36 determines that the packet stream is certainly corrupted or otherwise undesired or that threats are detected ("poor-confidence"), buffer 24 shunts the packets elsewhere, for example, either out of the firewall (e.g., to a "bit bucket" such as /dev/null, where they are discarded) or it shunts them elsewhere 26 for additional processing. If heuristic stage 36 is not certain as to the validity of the packets ("marginal-confidence"), buffer 24 releases the packets into complex firewall rule base 14 for processing. The output of complex firewall rule base 24 is buffer 40 (lines 32-58, Col. 3)]; and forward the data packets of the first type to a destination without testing by a virus scanning engine **[rating (i.e., an analysis of the packets 22 by heuristic stage 36 results in a high level of confidence that the packet stream does not contain threats that heuristic stage 36 is trained to detect), buffer 24 releases the packets into a**

secured channel 38 directly into network 30 (lines 30-43, Col. 39)] and forward the data packets of the second type of a virus scanning engine for testing [buffer 24 shunts the packets elsewhere, for example, either out of the firewall (e.g., to a "bit bucket" such as /dev/null, where they are discarded) or it shunts them elsewhere 26 for additional processing. If heuristic stage 36 is not certain as to the validity of the packets ("marginal-confidence"), buffer 24 releases the packets into complex firewall rule base 14 for processing (lines 51-57, Col. 39) If heuristic stage 36 rates packets 22 as either good-confidence or marginal-confidence, the packets are forwarded to another heuristic stage 44. Heuristic stage 44 is pre-trained to look for temporal and other anomalies in packet streams including, but not limited to, one or more of the following: temporal attack signatures, frequency analysis, in-transit packet modification, forged-packet indicators, out-of-band (OOB) communications, and/or covert channel communications (lines 59-67, Col. 39)]. Fink et al. and Joyce are analogous art because they are from similar technology relating to information security and packet scanning. It would have been obvious to one of ordinary skill in the art at the time of invention was made to combine the system disclosed in Fink et al. with Joyce since one

would have been motivated to provide methods and apparatus for a heuristic firewall that can learn from and adapt to data flowing through them to better mitigate such security threats (lines 34-37, Col. 1 from Joyce).

As per Claim 49, it is a method claim that corresponds to the apparatus claim 1. Therefore, Claim 49 is rejected for the same rationale as of Claim 1.

As per Claim 50, it is storage medium claim that corresponds to the apparatus claim 1. In addition, Fink et al. disclose a computer program stored on a storage medium **[The device comprising: (a) a memory for storing at least on instruction (lines 22-23, Col. 3). The method of the present invention could be described as a series of steps performed by a data processor, and as such could optionally be implemented as software, hardware, firmware, or a combination thereof (lines 63-66, Col. 3)]**. Therefore, Claim 50 is rejected for the same rationale as of Claim 1.

As per Claim 62, it is an apparatus claim that shares similar limitations as of claim 1. In addition, Fink et al. disclose memory and processor **[The device comprising: (a) a memory for**

storing at least on instruction (lines 22-23, Col. 3). The method of the present invention could be described as a series of steps performed by a data processor, and as such could optionally be implemented as software, hardware, firmware, or a combination thereof (lines 63-66, Col. 3)]. Therefore, Claim 62 is rejected for the same rationale as of Claim 1.

ii. *Referring to Claims 4, 53, and 58:*

As per Claim 4, Fink et al. and Joyce disclose the apparatus of claim 1 comprising:

wherein the classifying comprises determining that data packets of the first type contain real time data **[(lines 1-5, Abstract and lines 32-39, Col. 3)]**.

As per Claim 53, the rejection of claim 50 is incorporated. In addition, Claim 53 encompasses limitations that are similar to those of Claim 4. Therefore, it is rejected with the same rationale as of Claim 4.

As per Claim 58, the rejection of claim 49 is incorporated. In addition, Claim 58 encompasses limitations that are similar to those of Claim 4. Therefore, it is rejected with the same rationale as of Claim 4.

iii. *Referring to Claim 11:*

As per Claim 11, Fink et al. and Joyce disclose the apparatus of claim 1, further comprising a buffer configured to store the data packets of the second type while the virus scanning engine is testing the data packets to detect a virus **[(lines 39-65, Col. 2 from Joyce)]**.

iv. *Referring to Claims 32, 56, and 60:*

As per Claim 32, Fink et al. and Joyce disclose the apparatus of claim 1, wherein the firewall is configured to receive from a packet classification database, information defining the first and second types of data packets **[(lines 4-7 and lines 38-41, Col. 8 from Fink et al.)]**.

As per Claim 56, the rejection of claim 50 is incorporated. In addition, Claim 56 encompasses limitations that are similar to those of Claim 32. Therefore, it is rejected with the same rationale as of Claim 32.

As per Claim 60, the rejection of claim 49 is incorporated. In addition, Claim 60 encompasses limitations that are similar to those of Claim 32. Therefore, it is rejected with the same rationale as of Claim 32.

v. *Referring to Claim 33:*

As per Claim 33, Fink et al. and Joyce disclose the apparatus of claim 32, further comprising:

a virus scanning engine configured to receive from a virus detection database, programming information controlling the testing of the data packets of the second type by the virus scanning engine **[(lines 30-40, Col. 2 from Joyce)]**.

vi. *Referring to Claim 34:*

As per Claim 34, Fink et al. and Joyce disclose the apparatus of claim 1, further comprising:

a virus scanning engine configured to receive from a virus detection database, programming information controlling the testing of the data packets of the second type by the virus scanning engine **[(lines 30-40, Col. 2 from Joyce)]**.

vii. *Referring to Claim 40:*

As per Claim 40, Fink et al. and Joyce disclose the apparatus of claim 1, further comprising configured to alert the destination upon detection of a virus in the data packets **[(lines 61-67, Col. 4 from Joyce)]**.

viii. *Referring to Claim 41:*

As per Claim 41, Fink et al. and Joyce disclose the apparatus of claim 1 wherein the destination is a local area network **[protected network 12 (Fig. 1 from Fink et al.)]**.

ix. *Referring to Claim 42:*

As per Claim 42, Fink et al. and Joyce disclose the apparatus of claim 1 wherein the destination is a personal computer **[protected node 20 (Fig. 1 from Joyce)]**.

x. *Referring to Claim 43:*

As per Claim 43, Fink et al. and Joyce disclose the apparatus of claim 1, wherein the destination is a second network **[protected network 12 (Fig. 1 from Fink et al.)]**.

xi. *Referring to Claim 44:*

As per Claim 44, Fink et al. and Joyce disclose the apparatus of claim 1, wherein the first network is a wide area network **[external network 14 (Fig 1 from Fink et al.)]**.

xii. *Referring to Claim 45:*

As per Claim 45, Fink et al. and Joyce disclose the apparatus of claim 44, wherein the wide area network is the Internet **[External network 14 could optionally be the Internet, for example (lines 28-29, Col. 5 from Fink et al.)]**.

xiii. *Referring to Claim 46:*

As per Claim 46, Fink et al. and Joyce disclose the apparatus of claim 1, wherein the destination comprises an Internet service provider configured to connect coupled to a gateway,

a modem configured to connect to the Internet service provider, and one of a local area or personal computer configured to

connect to the modem **[(Fig. 1 from Fink et al.) and (lines 50-55, Col. 4 from Joyce)]**.

xiv. *Referring to Claim 47:*

As per Claim 47, Fink et al. and Joyce disclose the apparatus of claim 1, further comprising a virus scanning engine configured to decode the data packets during the testing of the data packets **[(lines 69-67, Col. 3 from Joyce) and (lines 4-11, Col. 7 from Fink et al.)]**.

xv. *Referring to Claim 48:*

As per Claim 48, Fink et al. and Joyce disclose the apparatus of claim 47, wherein the virus scanning engine is configured to function functions as a proxy for a destination processor configured to receive which receives the data packets **[(Fig. 1 from Fink et al.) and (lines 50-55, Col. 4 from Joyce)]**.

xvi. *Referring to Claim 61:*

As per Claim 61, Fink et al. and Joyce disclose the method of claim 49, wherein the classifying is performed by a firewall **[(lines 6-8, Col. 5; lines 65-67, Col. 6; lines 4-7, Col. 8 from Fink et al.)]**.

xvii. *Referring to Claim 65:*

As per Claim 65, Fink et al. and Joyce disclose the method of claim 49, wherein the classification is performed by a firewall **[(lines 30-40, Col. 2 and lines 32-58, Col. 3 from Joyce)]**.

5. Claims 5, 57, 59, and 63-64 are rejected under 35 U.S.C. 103(a) as being unpatentable over Fink et al. (U.S. Patent 6,496,935) and Joyce (U.S. Patent 6,519,703) and further in view of Lee (U.S. Patent 7,047,561).

   i. *Referring to Claims 5, 57, 59, and 63-64:*

   As per Claim 5, Fink et al. and Joyce disclose the apparatus of claim 4. Fink et al. and Joyce further disclose wherein the classifying comprises determining that data packets of the first type as in Claim 1. Fink et al. and Joyce do not expressly disclose the packets are part of an audio or video data stream. However, Lee discloses the packets are of video or audio content **[(lines 58-62, Col. 1 and lines 36-39, Col. 5 from Lee)]**. Fink et al., Joyce, and Lee are analogous art because they are from similar technology relating to Internet security regarding to data communications. It would have been obvious to one of ordinary skill in the art at the time of invention was made to modify Fink et al. and Joyce with Lee et al. to have the video or audio data in the packet(s) communicating in the network environment since one would be motivated to have a firewall for use in association with real-time Internet application (lines 7-8, Col. 1 in Lee).

   As per Claim 57, the rejection of claim 53 is incorporated. In addition, Claim 57 encompasses limitations that are similar to

those of Claim 5. Therefore, it is rejected with the same rationale as of Claim 5.

As per Claim 59, the rejection of claim 58 is incorporated. In addition, Claim 59 encompasses limitations that are similar to those of Claim 5. Therefore, it is rejected with the same rationale as of Claim 5.

As per Claim 63, the rejection of claim 62 is incorporated. In addition, Claim 63 encompasses limitations that are similar to those of Claim 5. Therefore, it is rejected with the same rationale as of Claim 5.

As per Claim 64, the rejection of claim 49 is incorporated. In addition, Claim 64 encompasses limitations that are similar to those of Claim 5. Therefore, it is rejected with the same rationale as of Claim 5.

6. Claims 6 and 54 are rejected under 35 U.S.C. 103(a) as being unpatentable over Fink et al. (U.S. Patent 6,496,935) and Joyce (U.S. Patent 6,519,703) and further in view of Lyle (U.S. Patent 6,886,012).

   i. *Referring to Claims 6 and 54:*

As per Claim 6, Fink et al. and Joyce disclose the apparatus of claim 1. Fink et al. and Joyce disclose the firewall as in Claim 1. Fink et al. and Joyce do not expressly disclose the remaining limitations of the claim. However, Lyle discloses stop reception of a data stream containing the data packets in response to an alert from the virus scanning engine **[(lines 28-34, Col. 14 from Lyle)]**. Fink et al., Joyce, and Lyle are analogous art because they are from similar technology relating to Internet security regarding to data communications. It would have been obvious to one of ordinary skill in the art at the time of invention was made to modify Fink et al. and Joyce with Lyle to have the various components in the gateway communicating with an alert message if the malicious code is detected, and to stop the data flow into the protected network in such a scenario since one would be motivated to have a way to share information about an attack, dynamically and without human intervention (lines 20-22, Col. 2 from Lyle).

As per Claim 54, the rejection of claim 50 is incorporated. In addition, Claim 54 encompasses limitations that are similar to those of Claim 6. Therefore, it is rejected with the same rationale as of Claim 6.

Response to Arguments

7. Applicant's amendment, filed on May. 28, 2008, has Claims 1, 4-6, 11, 32-34, 40-50, 53-54, and 56-63 as previously presented, and Claims 64-65 as newly added.

8. In view of Applicant's remark, filed on May. 28, 2008, argues that neither of the descriptions from the cited references, either separately or in combination, teaches or suggests classifying data packets into a first type which cannot contain a virus and packets of a second type which can contain a virus, a new reference by Joyce (U.S. Patent 6,519,703) is found and cited for rejecting the above-mentioned limitation. Please refer to the rejections above.

Conclusion

9. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.
    i. Chang et al. (U.S. Patent 6,950,874) disclose a method, system, apparatus, and computer program product are presented for management of resource leases within a distributed data processing system. A resource manager receives a lease request from a requester for a resource in which the lease request has a requested lease period. In response to receiving the lease request, the resource manager secures leases along a logical circuit of resources

through the distributed data processing system. The resource manager requests leases from other resource managers along the data path that comprises the logical circuit because use of the requested resource requires use of other resources. After securing leases on a logical circuit of resources, the resource manager returns a lease grant for the resource to the requester. If the system detects oversubscribed conditions and/or error conditions, the system can adjust the pending leases in an appropriate manner, such as terminating a lease, adjusting the lease period of a lease, and the like.

10. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Yin-Chen Shaw whose telephone number is 571-272-8593. The examiner can normally be reached on 8:15 to 4:15 M-F.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kristine Kincaid can be reached on 571-272-4063. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private

PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Y.C. Shaw

Aug. 28, 2008

/Kristine Kincaid/

Supervisory Patent Examiner, Art Unit 2139